NETWORK BLOCKING DEVICE FOR PAID INTERNET SERVICES

FIELD OF THE INVENTION

[0001] The present invention relates generally to pay per use Internet services and more particularly to systems that detect and verify the presence of network devices that share the Internet services on a mobile platform.

BACKGROUND OF THE INVENTION

[0002] Existing systems that receive pay per use Internet services commonly provide for sharing of a connection to the Internet services amongst multiple network devices for cost efficiency. For example, current Microsoft® Windows 98/2000 software technology allows users to share one Internet connection with multiple devices operating on a local network. More specifically, an Internet Connection Sharing function is provided in the Windows operating system such that one computer, hereinafter referred to as the Connection Sharing Computer, manages communications with the Internet services amongst a plurality of network devices, e.g. personal computers.

[0003] Generally, the Connection Sharing Computer establishes an initial, charged local area network (LAN) connection. The Connection Sharing Computer then serves as a controlling device for the LAN by providing Internet Protocol (IP) addresses and name resolution services for other computers on the LAN, hereinafter referred to as network devices. The network devices may then

access the Internet through the Connection Sharing Computer using private IP addressing translation. More specifically, when a network device on the network sends a request to the Internet, its private address is transmitted to the Connection Sharing Computer, and the Connection Sharing Computer then translates the IP address of the network device to its own Internet IP address and then sends it on to the Internet.

[0004] Private IP addressing translation occurs when automatic addressing is enabled, which allows the Connection Sharing Computer to use Dynamic Host Configuration Protocol (DHCP) to dynamically assign private IP address to all network devices on a LAN. A user may disable automatic addressing and statically assign an IP address to each network device on the LAN if DHCP is not used, which is common in many European countries. Further, the Connection Sharing Computer may also use sharing features to allow outside users on the Internet to access web sites, e-mail, and game servers that are hosted on the LAN.

[0005] To enable Internet Connection Sharing, all network devices on the LAN must have network adapters. One network device is the Connection Sharing Computer, which serves to establish a connection to the Internet using the method offered by the pay per use system, wherein an Internet connection wizard establishes the connection. Interfacing between the network devices is accomplished by assigning automatic private IP addresses for a LAN using TCP/IP (Transmission Control Protocol/Internet Protocol), which allows users to have a

small network with assigned unique IP addresses to the network adapter of the Connection Sharing Computer using a "LINKLOCAL" network.

[0006] Generally, LINKLOCAL network addresses begin with 169.254 and are used for private, internal addresses and thus are not valid for host computers that are not visible on the Internet. More specifically, the IP addresses cannot be used for computers linked by Internet Connection Sharing, as Internet Connection Sharing networks use addresses in the 192.168.0.xxx range. Accordingly, after a network adapter of a network device is assigned a LINKLOCAL network IP address, network devices can communicate, using TCP/IP protocol, with any other network device on the local network that uses the same addressing.

[0007] Despite extensive sophistication, a typical charge per use LAN system recognizes only the Connection Sharing Computer on the local network, due to the direct connection thereof. Accordingly, once the initial, charged Internet connection is established, Internet Connection Sharing is executed to configure the Connection Sharing Computer among other network devices. Further, the Internet Connection Sharing may also be used to configure external devices on the LAN to use file and print sharing to access resources from one another. Although the Internet Connection Sharing prevents access to the shared resource from the Internet, access by network devices is not monitored or blocked in network systems of the known art.

[0008] Accordingly, there remains a need in the art for a network architecture wherein access by network devices through a Connection Sharing

Computer may be detected and verified, and further blocked if necessary. A need further exists for a network architecture that is capable of detecting, verifying, and blocking access by network devices in a mobile platform network.

SUMMARY OF THE INVENTION

[0009] In one preferred form, the present invention provides a network architecture for blocking access to pay per use Internet services that comprises an Internet Protocol (IP) sniffer. Generally, the IP sniffer pings network devices (e.g., personal computers, laptops) to determine the presence of a network device in a local area network. If the IP sniffer detects a network device, the presence thereof is communicated to a server such that access to the Internet services by the network device may be blocked, if necessary.

[0010] Generally, the IP sniffer sweeps all possible combinations of addresses in a LINKLOCAL network to detect the addition of a network device on a port and reconfirms for a period of time to verify the presence thereof. Once the network device is confirmed, a signal is transmitted to the server such that the sharing violation may be further investigated or terminated. Preferably, the IP sniffer in one form is a module within a seat electronics box of a mobile platform (e.g., commercial aircraft), as described in greater detail below. Accordingly, the IP sniffer will constantly ping all network devices connected to each seat electronics box in a mobile platform.

[0011] Further areas of applicability of the present invention will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description and specific examples, while indicating the preferred embodiment of the invention, are intended for purposes of illustration only and are not intended to limit the scope of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The present invention will become more fully understood from the detailed description and the accompanying drawings, wherein:

[0013] Figure 1 is a flow diagram of a network architecture in accordance with the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0014] The following description of the preferred embodiments is merely exemplary in nature and is in no way intended to limit the invention, its application, or uses.

[0015] Referring to the drawings, a network architecture according to the present invention is illustrated and generally indicated by reference numeral 10 in Figure 1. As shown, the network architecture 10 is incorporated within a mobile platform environment, i.e. commercial air travel, wherein a router 12 receives and transmits Internet services via air-to-ground communications and transmits the Internet services to a server 14 and to a seat electronics box 16 within the mobile

platform. The Internet services are then transmitted through a local mini-hub 18, which transmits the services to a Connection Sharing Computer 20. The Connection Sharing Computer 20 then provides access to the Internet services for a plurality of network devices 22. As further shown, an IP sniffer 24 is incorporated within electronics of the seat electronics box 16 to detect, verify, and block access to pay per use Internet services by the network devices 22 as described in greater detail below.

[0016] Although the following detailed description is directed to a mobile platform such as a commercial aircraft, the invention is also applicable to other modes of mass transit such as ship, train, bus, among others. Accordingly, the reference to commercial aircraft should not be construed as limiting the scope of the present invention.

[0017] As shown, the router 12 communicates with ground equipment to receive the Internet services and to transmit requests for Internet services from the Connection Sharing Computer 20 and the network devices 22. The communications between the router 12 and the ground equipment generally comprises routing and forwarding, IP multicast forwarding, traffic control, point to point protocol over Ethernet (PPPoE) access server, network address translation (NAT), and network time protocol (NTP). The router 12 then transmits and receives proxied web accesses and domain name service (DNS) queries to and from the server 14.

[0018] The server 14 is generally a web server, a proxy server, a DNS server, an authorization server, and a default gateway for additional local networks. Further, the server 14 transmits and receives web accesses and DNS queries to and from the seat electronics box 16. Accordingly, the seat electronics box 16 generally comprises address resolution protocol (ARP) proxies, PPPoE relays, a dynamic host configuration protocol (DHCP) mini-server, simple network time protocol (SNTP), NAT for static laptops, and multicast stream control. Further, the seat electronics box 16 transmits and receives non-proxied traffic and PPPoe from a virtual private network (VPN) to and from the router 12.

[0019] As further shown, Internet services are transmitted to the local mini-hub 18 from the seat electronics box 16, preferably using dynamic host configuration (DHC). Generally, the Connection Sharing Computer 20 establishes an initial, charged local area network connection. The Connection Sharing Computer 20 then serves as a controlling device for the network by providing Internet Protocol (IP) addresses and name resolution services for the network devices 22. The network devices 22 may then access the Internet through the Connection Sharing Computer 20 using private IP addressing translation. More specifically, when a network device 22 on the network sends a request to the Internet, its private address is transmitted to the Connection Sharing Computer 20, and the Connection Sharing Computer 20 then translates the IP address of the network device to its own Internet IP address and then sends it on to the Internet.

[0020] Accordingly, the IP sniffer 24 is incorporated within the seat electronic box 16 to detect, verify, and if necessary, block access to the Internet services by the network devices 22. The IP sniffer 24 constantly pings all of the network devices 22 connected to each seat electronics box 16 of a mobile platform for any IP address in the 169.254.X.X range. Since there are only 256 x 256 possible combinations, or 65,536 in total, a full sweep of the possible IP addresses may be completed approximately every 5 minutes to detect the addition of a network device 22 on a port.

[0021] Once a return ping is detected, the IP sniffer 24 reconfirms the connection by the network device 22 for approximately one more minute to verify the presence thereof. When a network device 22 is confirmed, the seat electronics box 16 sends a signal to the server 12, where either on-board personnel may be flagged to investigate the possible sharing violation or the network architecture 10 may terminate service to the port being shared by the network device 22. Accordingly, access to pay per use Internet services by network devices is monitored and controlled by the network architecture 10 of the present invention.

[0022] The description of the invention is merely exemplary in nature and, thus, variations that do not depart from the substance of the invention are intended to be within the scope of the invention. Such variations are not to be regarded as a departure from the spirit and scope of the invention.